UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/033,034	12/27/2001	Shigeki Kamiya	450100-03254.1	8632

20999 7590 06/24/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/033,034	KAMIYA ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-20** have been examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. **Claims 6-20** are rejected under 35 U.S.C. 102(b) as being anticipated by **Eskicioglu Ahmet.** (hereinafter referred as **Ahment**) (Submitted IDS)(International Publication number: **WO 99/30499, publication date 06/17/1999**)

5. **As per claim 6 Ahment** a downstream system usable in an electronic data delivery system to output content, comprising: A decryption server to which encrypted digital data is delivered, said decryption server including: a decryption unit for decrypting said encrypted digital data;[Page 2, lines 11-13](**receiving a scrambled/encoded signal**

from a source and generating a descrambling key in response to received signal and descrambling/decrypting the data using the descrambling key.]

- A scramble control unit for locally generating a scramble key and a descramble key if the delivered digital data is successfully decrypted; [Page 2, line 15 & page 2, lines 11-12] (**generating locally a scrambling key in response to said received data as explained on page 2, line 15 and generating locally a descrambling key as explained on page 2, lines 11-12**)

- A content decoder for decoding the decrypted digital data to output restored digital data and a scrambler for scrambling said restored digital data with the locally generated scramble key;[Page 2, line 15-17] (**generating a scrambling key in response to said received data and scrambling said descrambled/decoded restored digital data/signal using the locally generated scrambling key to generate a re-scrambled signal**) and

An output device coupled to said decryption server and including:

- A descrambler for descrambling the scrambled, restored digital data with said descramble key generated in said decryption server; and a signal processor for processing the descrambled digital data to a predetermined format and outputting the processed digital data as said content. [Page 2, line 17-18; page 1, lines 32-38] (**As explained on page 1, lines 32-38, the external source/output device/host device/display device or a set top box as explained on page 1, lines 37-38 which is used to receive data from the smart card/a conditional access device in-the-clear is not secure and Ahment invention is mainly done to solve this problem. According to Ahment instead of sending signal/data in-the-clear, the external device/output device receives a re-scrambled/encoded date as explained on page**

2, line 17-18 and the external source/output device/host device/display device or a set top box will inherently descramble the re-scrambled & restored digital data using the same/corresponding key and it will inherently be processed in a predetermined format and finally the outputting of the content will be followed.]

6. **Claims 7-20** are rejected for the same reasons as claim 6 above, as they are part and parcel of claim 6 and recites similar limitation

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claim 1-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Eskicioglu Ahmet.** (hereinafter referred as **Ahment**) (Submitted IDS)(International Publication number: wo 99/30499, publication date 06/17/1999) in view of **Schneier**: (Submitted IDS) "Applied cryptography". (hereinafter referred to as **Schneier**)

9. **As per claim 1 Ahment** discloses a method of multipoint delivery of encoded digital data from an upstream system to specific destinations in a downstream system, comprising the steps of:

- Encrypting digital data by the use in said upstream system of an encryption key delivering said encrypted, encoded digital data; receiving said encrypted, encoded digital data and encryption key information by a decryption server at said downstream system, said decryption server being accessed only by authorization;[Page 2, lines 10-11]**(receiving a scrambled/encoded signal from a source and as explained on page 2, lines 11-12, signal used/key information to construct the key is also received from the source)**

- Using the restored key to decrypt and decode the received digital data; [Page 2, lines 11-12] **(generating a descrambling/restored key in response to said received signal and descrambling & decoding the data/signal)**

- Locally generating a scramble key and a descrambling key [Page 2, line 15 & page 2, lines 11-12] **(generating a scrambling key in response to said received data as explained on page 2, line 15 and generating descramble key as explained on page 2, lines 11-12)**

- Using the locally generated scramble key to scramble said restored digital data;[Page 2, line 15-17] **(generating a scrambling key in response to said received data and scrambling said descramble/decoded signal using the scrambling key to generate a re-scrambled signal)**

- Descrambling the scrambled digital data by an output device at said downstream system using the descramble key generated by said decryption server, said output device being accessed only by authorization; and outputting from said output

device the descrambled digital data in a predetermined output format. [Page 2, line 17-18; page 1, lines 32-38] **(As explained on page 1, lines 32-38, the external source/output device/host device/display device or a set top box as explained on page 1, lines 37-38 which is used to receive data from the smart card/a conditional access device in-the-clear is not secure and Ahment invention is mainly done to solve this problem. According to Ahment instead of sending signal/data in-the-clear, the external device/output device receives a re-scrambled/encoded date as explained on page 2, line 17-18 and the external source/output device/host device/display device or a set top box will inherently descramble the re-scrambled digital data using the same/corresponding key and it will inherently be processed in a predetermined format and finally the outputting of the content will be followed.]**

Ahment does not explicitly disclose

- Generating, on the basis of said encryption key, a plurality of pieces of key information, respective pieces of said key information being specific to each of said specific destinations; delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes that differ from routes used to deliver said digital data and that differ from each other; restoring said encryption key based on the received pieces of key information;

However, in the field of endeavor **Schneier discloses**, discloses

Generating, on the basis of said encryption key, a plurality of pieces of key information, respective pieces of said key information being specific to each of said specific destinations; delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes that differ from routes used to deliver

said digital data and that differ from each other; restoring said encryption key based on the received pieces of key information;[Page 176, lines 34-last line; page 177, lines 1-2; page 177, line 1-16; and figure 8.2 on page 177]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ the features of delivering partial key and restoring the key based on the pieces of key information and furthermore delivering over plurality of delivery routes that differ from routes used to deliver the digital data as per teachings of **Schneier** in to the method as taught by **Ahment** in order to securely protect the key from being illegally reconstructed and protect the content from illegally decrypted.

10. **Claims 2-5** are rejected for the same reasons as claim 1 above, as they are part and parcel of claim 1and recites similar limitation.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on. The fax phone number for the organization where this application or proceeding is assigned is 571-272-3799.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
06/15/2005

Gilberto Barron Jr
GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100